

A characteristic 2 recurrence related to U_5 , with a Hecke algebra application

Paul Monsky

Brandeis University, Waltham MA 02454-9110, USA. monsky@brandeis.edu

Abstract

In arXiv:1603.03910 [math.NT] we introduced some C_n in $Z/2[t]$ defined by a linear recurrence and showed that each C_n , $n \equiv 0 \pmod{4}$, is a sum of C_k , $k < n$. Combining this with results from arXiv:1508.07523 [math.NT] we proved that the space K , consisting of those odd mod 2 modular forms of level $\Gamma_0(3)$ that are annihilated by the operator $U_3 + I$, has a basis $m_{i,j}$ “adapted to T_7 and T_{13} ” in the sense of Nicolas and Serre. (And so the “completed shallow Hecke algebra” attached to K is a power series ring in T_7 and T_{13} .)

This note derives analogous results in level $\Gamma_0(5)$. Now $U_3 + I$ is replaced by $U_5 + I$, and the operators T_7 and T_{13} by T_3 and T_7 . In place of level $\Gamma_0(3)$ results from 1508.07523, we use level $\Gamma_0(5)$ results from arXiv:1603.07085 [math.NT]. A linear recurrence again plays the key role. Now $C_{n+6} = C_{n+5} + (t^6 + t^5 + t^2 + t)C_n + t^n(t^2 + t)$, $C_0 = 0$, $C_1 = C_2 = 1$, $C_3 = t$, $C_4 = t^2$, $C_5 = t^4 + t^2 + t$, and we prove that each C_n , $n \equiv 0 \text{ or } 2 \pmod{6}$ is a sum of C_k , $k < n$.

1 Introduction. The polynomials C_n

The first 4 sections of this note, apparently unconnected with modular forms, consist of calculations in a polynomial ring $Z/2[r]$ that might seem unmotivated. The motivation in fact comes from [4]. In that note I introduce commuting Hecke operators $T_p : Z/2[[x]] \rightarrow Z/2[[x]]$, p an odd prime, together with a subspace, $M(\text{odd})$, of $Z/2[[x]]$ stabilized by the T_p , $p \neq 5$. $M(\text{odd})$ is the “space of odd mod 2 modular forms of level $\Gamma_0(5)$,” and contains the reductions F and G of the expansions at infinity of $\Delta(z)$ and $\Delta(5z)$. I construct subspaces $N2 \supset N1$ of $M(\text{odd})$, also stabilized by these T_p , and write $N2/N1$ as a direct sum $N2a \oplus N2b$. I then show that $N2a$ and $N2b$ are stabilized by the T_p , $p \equiv 1, 3, 7, 9 \pmod{20}$ and that $N2a$ has a basis $m_{i,j}$ “adapted to T_3 and T_7 ” in the sense of Nicolas and Serre, with $m_{0,0} = F$.

Now let $U_5 : Z/2[[x]] \rightarrow Z/2[[x]]$ be the map $\sum c_n x^n \rightarrow \sum c_{5n} x^n$. It’s easy to

see that U_5 stabilizes $M(\text{odd})$ and commutes with the T_p , $p \neq 5$. So the kernel, K , of $U_5 + I$ acting on $M(\text{odd})$ is stabilized by *all* T_p , $p \neq 5$ (or 2), and there is a shallow Hecke algebra attached to K , generated by these T_p .

The goal of this note is to show that K , like $N2a$, has a basis $m_{i,j}$ adapted to T_3 and T_7 ; now $m_{0,0} = F + G$. In fact we show that $K \subset N2$, and that the projection map from $N2$ to $N2a$ maps K bijectively to $N2a$. Since the projection map preserves the action of T_3 and T_7 , K has the desired basis. A consequence is that there is a faithful action of $Z/2[[X, Y]]$ on K with X and Y acting by T_3 and T_7 , and that each $T_p : K \rightarrow K$, $p \neq 2$ or 5 is multiplication by an element of (X, Y) . In a more elaborate language this says that the “completed shallow Hecke algebra” attached to K is a power series ring in T_3 and T_7 .

Now the statement that $K \subset N2$ and projects bijectively from $N2/N1$ to $N2a$ can be phrased without invoking modular forms; it is just algebra in a polynomial ring. Namely there is an r in $Z/2[[x]]$ with $r^2 + r = F + G$, and using results from [4] one can show that the principal actors, F , G , $M(\text{odd})$, U_5 , K , $N1$, $N2a$, $N2b$ can be defined purely in terms of this r . In sections 1–4 we take r to be an indeterminate over $Z/2$, and define these principal actors. (But U_5 will be called U .) We then show that $K \subset N2$ and that $K \rightarrow N2a$ is bijective. In section 5, the actors drop their masks, revealing their connections with modular forms, and we conclude that the kernel of $U_5 + I$ acting on $M(\text{odd})$ has the desired basis.

Here’s a preview of the section 1–4 calculations in $Z/2[r]$. F and G are $r(r+1)^5$ and $r^5(r+1)$. $M(\text{odd})$ is spanned by the $(r^2 + r)r^{2n}$, and $U : Z/2[r] \rightarrow Z/2[r]$ is a certain operator with $U(Gf) = FU(f)$. In section 1 we show that $U + I$ takes $(r^2 + r)r^{2n}$ to $(r^2 + r)C_n(r^2)$ where the C_n lie in $Z/2[t]$ and satisfy a certain recurrence. In section 2 we use this recurrence to show that each C_n with $n \equiv 0$ or $2 \pmod{6}$ is a sum of C_k , $k < n$, and consequently that there are g_n of degree n , one for each $n \equiv 0$ or $2 \pmod{6}$, with $f_n = (r^2 + r)g_n(r^2)$ forming a basis of K . In Theorem 3.5 of section 3 we show that these g_n may be chosen to satisfy somewhat more stringent conditions. In section 4 we re-examine the arguments of section 2. We construct $Z/2[G^2]$ submodules $N1$ and $N2$ of $M(\text{odd})$ with bases $\{G\}$ and $\{G, F, F^2G, F^3, F^4G\}$ and show that $K \subset N2$. We then define certain J_k , $(k, 10) = 1$, in $N2$ with $J_{k+10} = G^2J_k$. $N2a$ and $N2b$ are the subspaces of $N2/N1$ spanned by the J_k with $k \equiv 1, 3, 7, 9 \pmod{20}$ and the J_k with $k \equiv 11, 13, 17, 19 \pmod{20}$. We use Theorem 3.5 to get information about the image of f_n under the composite map $N2 \rightarrow N2/N1 \rightarrow N2a$, and establish the desired bijection.

Definition 1.1 F and G in $Z/2[r]$ are $r(r+1)^5$ and $r^5(r+1)$. Note that $F + G = r(r+1)$ and $(F + G)^6 + FG = 0$.

Definition 1.2 $\sigma : Z/2[r] \rightarrow Z/2[r]$ is semi-linear if it is $Z/2$ -linear, and $\sigma(Gf) = F\sigma(f)$.

Since a basis of $Z/2[r]$ as module over $Z/2[G] = Z/2[r^6 + r^5]$ is $1, r, r^2, r^3, r^4, r^5$, a semi-linear map is determined by the images of these 6 elements. And for any choice of 6 elements to be images there is a corresponding semi-linear map.

Definition 1.3 $U : Z/2[r] \rightarrow Z/2[r]$ is the semi-linear map taking $1, r, r^2, r^3, r^4$ and r^5 to $1, r, r^2, r^3 + r^2 + r, r^4$ and $r^5 + r^4 + r$. Since $U(1) = 1$, $U(G^n) = F^n$.

Lemma 1.4 $U(f^2) = (U(f))^2$

Proof Since $1, r, r^2, r^3, r^4, r^5$ form a basis of $Z/2[r]$ as $Z/2[G]$ -module, and $U(G) = F$, it suffices to prove this when f is $1, r, r^2, r^3, r^4$ or r^5 . The result is immediate for $1, r$ and r^2 . And:

$$\begin{aligned} r^6 &= G + r^5. \text{ So } U(r^6) = F + (r^5 + r^4 + r) = r^6 + r^4 + r^2 = (U(r^3))^2. \\ r^8 &= (r^2 + r)G + r^6. \text{ So } U(r^8) = (r^2 + r)F + r^6 + r^4 + r^2 = r^8 = (U(r^4))^2. \\ r^{10} &= (r^4 + r^3)G + r^8. \text{ So } U(r^{10}) = (r^4 + r^3 + r^2 + r)F + r^8 \\ &= r^2(r + 1)^8 + r^8 = r^{10} + r^8 + r^2 = (U(r^5))^2. \end{aligned}$$

□

Lemma 1.5

- (a) $U(r^{n+6}) = U(r^{n+5}) + (r^6 + r^5 + r^2 + r)U(r^n)$.
- (b) $U((r^2 + r)r^{2n}) = (r^2 + r)A_n(r^2)$ for some A_n in $Z/2[t]$.

Proof $r^6 = r^5 + G$. Multiplying by r^n , applying U and using semi-linearity, we get (a). Now $U(r^2 + r) = r^2 + r$, while $U(r^4 + r^3) = (r^2 + r)(r^2 + 1)$. So for $n = 0$ and $n = 1$ we have (b) with $A_0 = 1$ and $A_1 = t + 1$. Suppose $n \geq 2$. By (a), $U((r^2 + r)r^{2n}) = (r^6 + r^5 + r^2 + r)U(r^{2n-4})$, which by Lemma 1.4 is $(r^2 + r)(r^4 + 1)(U(r^{n-2}))^2$. So if we write $U(r^{n-2})$ as $g(r)$, we get (b) with $A_n = (t^2 + 1)g(t)$. □

Lemma 1.6 Let A_n be as in Lemma 1.5. Then:

- (a) $A_{n+6} = A_{n+5} + (t^6 + t^5 + t^2 + t)A_n$.
- (b) $A_0, A_1, A_2, A_3, A_4, A_5$ are $1, t + 1, t^2 + 1, t^3 + t, t^4 + t^2, t^5 + t^4 + t^2 + t$.

Proof $r^{12} = r^{10} + G^2$. Multiplying by $(r^2 + r)r^{2n}$, applying U , and then dividing by $r^2 + r$ we find that $A_{n+6}(r^2) = A_{n+5}(r^2) + (r^{12} + r^{10} + r^4 + r^2)A_n(r^2)$, giving (a). A_0 and A_1 are 1 and $t + 1$. When $n = 2, 3, 4, 5$, then $U(r^{n-2})$ is $1, r, r^2, r^3 + r^2 + r$, and we use the final sentence in the proof of Lemma 1.5 to get (b). □

Definition 1.7 C_n in $Z/2[t]$ is $A_n + t^n$, with A_n as in Lemma 1.5.

Theorem 1.8

- (a) $C_{n+6} = C_{n+5} + (t^6 + t^5 + t^2 + t)C_n + t^n(t^2 + t)$.
- (b) $C_0, C_1, C_2, C_3, C_4, C_5$ are $0, 1, 1, t, t^2, t^4 + t^2 + t$.
- (c) $U + I$ takes $(r^2 + r)r^{2n}$ to $(r^2 + r)C_n(r^2)$.

Proof (a) and (b) follow from (a) and (b) of Lemma 1.6, while (c) comes from Lemma 1.5(b). \square

Lemma 1.9

- (a) If $n \equiv 1$ or $5 \pmod{6}$, degree $C_n = n - 1$.
- (b) If $n \equiv 3$ or $4 \pmod{6}$, degree $C_n = n - 2$.
- (c) If $n \equiv 0$ or $2 \pmod{6}$, degree $C_n \leq n - 2$.

Proof For $n \leq 5$ we use Theorem 1.8(b). To show, by induction, that the results hold for $n + 6$, look at (a) of Theorem 1.8. The induction assumption tells us that the first term on the right has degree $\leq n + 4$, and the same is true for the last term. When $n \equiv 1$ or $5 \pmod{6}$, the middle term, by the induction assumption, has degree $6 + (n - 1) = n + 5$, so C_{n+6} has degree $n + 5$. When $n \equiv 0$ or $2 \pmod{6}$, the middle term has degree $\leq 6 + (n - 2) = n + 4$, so degree $C_{n+6} \leq n + 4$. Finally when $n \equiv 3$ or $4 \pmod{6}$, the first and last terms on the right have degree $\leq n + 3$ while the middle term has degree $6 + (n - 2) = n + 4$. So C_{n+6} has degree $n + 4$. \square

Lemma 1.10 If C_n is a $Z/2$ -linear combination of C_k , $k < n$, then $n \equiv 0$ or $2 \pmod{6}$.

Proof If $n \equiv 1$ or $5 \pmod{6}$, then C_n has degree $n - 1$, while each C_k , $k < n$, has degree $< n - 1$. Similarly when $n \equiv 3$ or $4 \pmod{6}$, C_n has degree $n - 2$, while each C_k , $k < n$, has degree $< n - 2$. \square

2 A key property of the C_n

We'll prove a converse, Theorem 2.11, to Lemma 1.10; if $n \equiv 0$ or $2 \pmod{6}$, then C_n is a $Z/2$ -linear combination of C_k , $k < n$. (This is one of several related conjectures about recurrences found in [1]. Peter Müller, in a short computer calculation, showed it to be true for $n < 10,000$.)

Lemma 2.1 U takes $F + G$, $(F + G)^3$ and $(F + G)^5$ to $F + G$, $(F + G)^3$ and $(F + G)^5 + F$.

Proof Since $F + G = r^2 + r$, the first result holds. Also, $U(F + G)^3 = U(r^6 + r^5 + r^4 + r^3) = U(G + r^4 + r^3) = F + r^4 + r^3 + r^2 + r = r^6 + r^5 + r^4 + r^3$. Finally, $(F + G)^5 = (r^2 + r)^5 = (r^4 + 1)G$; U takes this to $r^4F + F = (r^2 + r)^5 + F$. \square

Lemma 2.2 U takes $1, F, F^2, F^3, F^4, F^5$ to $1, G, G^2, G^3, G^4, G^5 + F$.

Proof Since U fixes $F + G$, and $U(G) = F$, $U(F)$ must be G . By Lemma 1.4, $U(F^2) = G^2$, $U(F^4) = G^4$. Since U is semi-linear it interchanges F^2G and FG^2 , as well as F^4G and FG^4 . Now $F^3 + G^3 = (F + G)^3 + F^2G + FG^2$. Lemma 2.1 then shows that U fixes $F^3 + G^3$, and since $U(G^3) = F^3$, $U(F^3) = G^3$. Similarly, since $F^5 + G^5 = (F + G)^5 + F^4G + FG^4$, Lemma 2.1 shows that U takes $F^5 + G^5$ to $F^5 + G^5 + F$, and since $U(G^5) = F^5$, $U(F^5) = G^5 + F$. \square

Lemma 2.3 Let α be the $Z/2$ -linear isomorphism $Z/2[F] \rightarrow Z/2[G]$ with $\alpha(F^n) = G^n$. Then if P_n is either $\alpha(F^n) = G^n$ or $U(F^n)$,

$$(\star) \quad P_{n+6} + F^2P_{n+4} + F^4P_{n+2} + F^6P_n + FP_{n+1} = 0.$$

Proof As we saw in Definition 1.1, $(F + G)^6 + FG = 0$. Multiplying by G^n and expanding we get (\star) with $P_n = G^n = \alpha(F^n)$. Multiplying instead by F^n , and applying the semi-linear operator U , we get (\star) with $P_n = U(F^n)$. \square

Definition 2.4 For f in $Z/2[F]$, $T(f) = U(f) + \alpha(f)$.

Lemma 2.5

- (a) T takes $1, F, F^2, F^3, F^4$ and F^5 to $0, 0, 0, 0, 0$ and F .
- (b) T stabilizes $Z/2[F]$. In fact, $T(F^n)$ is a sum of F^k with each $k \equiv n \pmod{2}$, and $\leq n - 4$.

Proof (a) is immediate from Lemma 2.2, and in particular the second assertion in (b) holds for $n \leq 5$. Now let $P_n = T(F^n)$. By Lemma 2.3 the P_n satisfy the recursion (\star) above. An induction on n completes the proof of (b). \square

Lemma 2.6 Let u_0, u_1, u_2, u_4, u_5 be $F + G, (F + G)^3 + G, G, (F + G)^2G, (F + G)^4G + (F + G)FG$. Then the u_i are linearly independent over $Z/2[G]$ and $u_i = (r^2 + r)g(r^2)$ for some g of degree i .

Proof Since $1, F, F^2, F^3$ and F^4 are linearly independent over $Z/2[G]$, the first assertion holds. The g corresponding to u_0 and u_2 are evidently 1 and t^2 . Since $(F + G)^2 = r^4 + r^2$, the g corresponding to u_1 is $(t^2 + t) + t^2 = t$. Since $(F + G)G = r^8 + r^6$, the g corresponding to u_4 is $t^4 + t^3$. Since $G(F + G)^3 + FG = (r^6 + r^5)(r^4 + r^3 + r^2 + r) = r^{10} + r^6$, the g corresponding to u_5 is $t^5 + t^3$. \square

We now fix $m \geq 0$.

Definition 2.7 L is the space spanned by the $u_i G^{2n}$ with $i \in \{0, 1, 2, 4, 5\}$ and $0 \leq n \leq m$. L^* consists of the $(r^2 + r)g(r^2)$, where g in $Z/2[t]$ has degree $\leq 6m + 5$.

Lemma 2.8 L has dimension $5m + 5$, and $L \subset L^*$.

Proof The linear independence of the u_i over $Z/2[G]$ gives the first result. Since $G^{2n} = (r^{12} + r^{10})^n$, and $n \leq m$, the last part of Lemma 2.6 shows that $L \subset L^*$. \square

Remark Let $M(\text{odd})$ consist of all elements of $Z/2[r]$ of the form $(r^2 + r)g(r^2)$, g in $Z/2[t]$. Lemma 1.5(b) shows that U stabilizes $M(\text{odd})$. Also, if the A_n are as in Lemma 1.5, then Lemma 1.6 and an induction show that the degree of A_n is $\leq n$, and it follows that U stabilizes L^* . (But when $m \geq 2$, U does not stabilize L . For $G^5 = G^4 u_2$ is in L , but $U(G^5) = F^5$ is not even a $Z/2[G]$ -linear combination of u_0, u_1, u_2, u_4 and u_5 .)

Lemma 2.9 For $0 \leq i \leq 4$, $(U + I)^2 = U^2 + I$ maps $F^i G^k$ to $F^i T(F^k)$.

Proof $U(F^i G^k) = F^k U(F^i)$; since $i \leq 4$ this is $F^k G^i$. Then $U^2(F^i G^k) = F^i U(F^k) = F^i (G^k + T(F^i))$, and the result follows. \square

Theorem 2.10 Let K_m be the kernel of $U + I : L^* \rightarrow L^*$. (The remark above shows that $U + I$ stabilizes L^* .) Then the dimension of K_m is $\geq 2m + 2$.

Proof Each $u_i G^{2n}$ with $0 \leq n \leq m$ is a sum of $F^i G^k$ where $i \leq 4$ and $i + k$ is both odd and $\leq 2m + 5$; see the definition of the u_i . By Lemma 2.9 the image of any of these elements under $(U + I)^2$ is a sum of $F^i T(F^k)$ with $i + k$ odd and $\leq 2m + 5$. By Lemma 2.5(b), each such $F^i T(F^k)$ is in the space spanned by the F^n with n odd and $\leq 2m + 1$. It follows that the image of L under $(U + I)^2$ has dimension $\leq m + 1$, and that the dimension of the kernel is $\geq (5m + 5) - (m + 1) = 4m + 4$. Since $L \subset L^*$, $(U + I)^2 : L^* \rightarrow L^*$ has a kernel whose dimension is $\geq 4m + 4$, and the dimension of K_m is $\geq 2m + 2$. \square

Theorem 2.11 If $n = 6m$ or $6m + 2$, C_n is a $Z/2$ -linear combination of C_k , $k < n$.

Proof Let L and L^* be as in Definition 2.7, and K_m be as in Theorem 2.10. Suppose $f = (r^2 + r)g(r^2)$ is a non-zero element of K_m . Write g as $t^j +$ a sum of t^k with $k < j$. Applying $U + I$ and using Theorem 1.8(c) we find that C_j is the sum of the corresponding C_k . So by Lemma 1.10, $j \equiv 0$ or $2 \pmod{6}$. Since $j \leq 6m + 5$, the degree, $2j + 2$, of f in r is 2 or 6 mod 12 and lies in $[0, 12m + 12]$; this restricts us to $2m + 2$ possible degrees. Now K_m admits a $Z/2$ -basis of elements with distinct degrees in r . We've just shown that only the $2m + 2$ integers in $\{2, 6, 14, 18, \dots, 12m + 2, 12m + 6\}$ can be degrees. Since the dimension of K_m is $\geq 2m + 2$, each of these degrees does occur, and in

particular there's an $f = (r^2 + r)g(r^2)$ in K_m with the degree, n , of g equal to $6m$ (and also such an f with the degree of g equal to $6m + 2$). Write g as $t^n +$ (a sum of t^k with $k < n$). Applying $U + I$ and using Theorem 1.8(c) we find that C_n is the sum of the corresponding C_k . \square

Corollary 2.12 *Let $\varphi : Z/2[t] \rightarrow Z/2[t]$ be the $Z/2$ -linear map taking t^k to C_k . Then the kernel of φ has a basis consisting of g_n of degree n , one for each $n \equiv 0$ or $2 \pmod{6}$.*

Proof Immediate from Lemma 1.10 and Theorem 2.11. \square

Corollary 2.13 *Let K be the kernel of $U + I : M(\text{odd}) \rightarrow M(\text{odd})$. Then the $(r^2 + r)g_n(r^2)$, g_n as in Corollary 2.12, are a $Z/2$ -basis of K .*

Proof Theorem 1.8(c) shows that $(r^2 + r)g(r^2)$ is in K if and only if $\varphi(g) = 0$. \square

3 More about the g_n

In Corollary 2.12 we introduced certain g_n in $Z/2[t]$, $n \equiv 0$ or $2 \pmod{6}$. We now use the recursion for the C_n to show that the g_n can be chosen to satisfy certain further conditions. If g is in $Z/2[t]$, $g = O(t^m)$ will be shorthand for “the degree of g is $\leq m$ ”.

Lemma 3.1

- (a) *If $n \geq 24$, $C_n = t^{24}C_{n-24} + O(t^{n-5})$. When n is even, $n - 5$ can be replaced by $n - 6$.*
- (b) *If $n \geq 48$, $C_n = t^{48}C_{n-48} + O(t^{n-9})$.*

Proof The recursion of Theorem 1.8 shows that $C_n = C_{n-4} + (t^{24} + t^{20} + t^8 + t^4)C_{n-24} + t^{n-24}(t^8 + t^4)$. Since C_m is $O(t^{m-1})$ and is $O(t^{m-2})$ for even m , each term on the right other than $t^{24}C_{n-24}$ is $O(t^{n-5})$, and indeed is $O(t^{n-6})$ for even n . Similarly we use the fact that $C_n = C_{n-8} + (t^{48} + t^{40} + t^{16} + t^8)C_{n-48} + t^{n-48}(t^{16} + t^8)$ to get (b). \square

Lemma 3.2

- (a) *When $n \equiv 0 \pmod{12}$, $C_n = O(t^{n-4})$.*
- (b) *When $n \equiv 2 \pmod{12}$, $C_n + C_{n-1} = O(t^{n-4})$.*
- (c) *When $n \equiv 8 \pmod{24}$, $C_n = O(t^{n-6})$.*
- (d) *When $n \equiv 20 \pmod{24}$, $C_n + C_{n-2} = O(t^{n-6})$.*

Proof C_0 and C_{12} are easily seen to be 0 and $t^8 + t^4 + t^2$. So (a) holds for $n = 0$ and 12. Suppose $n \geq 24$ and $0 \pmod{12}$. Then $C_n = t^{24}C_{n-24} + O(t^{n-5})$; by induction this is $O(t^{n-4})$. Also, $C_2 + C_1 = 0$, while $C_{14} + C_{13}$ has degree 10. So (b) holds when $n = 2$ or 14. If $n \geq 26$ is $2 \pmod{12}$, then $C_n + C_{n-1} = t^{24}(C_{n-24} + C_{n-25}) + O(t^{n-5})$, which by induction is $O(t^{n-4})$, and we get (b). Similarly, using the fact that $C_8 = t^2$ and that $C_{20} + C_{18}$ has degree 8, we use the second sentence in Lemma 3.1(a) to establish (c) and (d) by induction. \square

Lemma 3.3

- (a) When $n \equiv 6 \pmod{24}$, $C_n + C_{n-1} + C_{n-2} + C_{n-3} + C_{n-4} + C_{n-5} = O(t^{n-8})$.
When $n \equiv 6 \pmod{24}$, $C_n + C_{n-1} + C_{n-2} + C_{n-3} = O(t^{n-8})$.
- (b) When $n \equiv 18 \pmod{24}$, $C_n + C_{n-1} = O(t^{n-8})$.
When $n \equiv 18 \pmod{24}$, $C_n + C_{n-1} + C_{n-4} + C_{n-5} = O(t^{n-8})$.

Proof Lemma 3.2(b) shows that $C_{n-4} + C_{n-5} = O(t^{n-8})$, so it's enough to check the first parts of (a) and (b). These first parts are verified using Lemma 3.1(b), an induction, and the following observations: $C_6 + C_5 + C_4 + C_3 + C_2 + C_1 = 0$, $C_{30} + C_{29} + C_{28} + C_{27} + C_{26} + C_{25}$ has degree 22, $C_{18} + C_{17}$ has degree 8 and $C_{42} + C_{41}$ has degree 34. \square

Lemma 3.4 *The g_n of Corollary 2.12 can be chosen so that:*

- (a) When $n \equiv 0 \pmod{12}$, $g_n = t^n + O(t^{n-2})$.
- (b) When $n \equiv 2 \pmod{12}$, $g_n = t^n + t^{n-1} + O(t^{n-2})$.
- (c) When $n \equiv 8 \pmod{24}$, $g_n = t^n + O(t^{n-4})$.
- (d) When $n \equiv 20 \pmod{24}$, $g_n = t^n + t^{n-2} + O(t^{n-4})$.
- (e) When $n \equiv 6 \pmod{48}$, $g_n = t^n + t^{n-1} + t^{n-2} + t^{n-3} + t^{n-4} + t^{n-5} + O(t^{n-6})$.
- (f) When $n \equiv 18 \pmod{48}$, $g_n = t^n + t^{n-1} + O(t^{n-6})$.
- (g) When $n \equiv 30 \pmod{48}$, $g_n = t^n + t^{n-1} + t^{n-2} + t^{n-3} + O(t^{n-6})$.
- (h) When $n \equiv 42 \pmod{48}$, $g_n = t^n + t^{n-1} + t^{n-4} + t^{n-5} + O(t^{n-6})$.

Proof I'll treat (g)—the other parts are handled similarly. The φ of Corollary 2.12 taking t^n to C_n gives a map:

$$\bar{\varphi} : \frac{\text{polynomials of degree } \leq n}{\text{polynomials of degree } \leq n-6} \rightarrow \frac{\text{polynomials of degree } \leq n-2}{\text{polynomials of degree } \leq n-8}$$

By Lemma 3.3, $\bar{\varphi}$ annihilates $t^n + t^{n-1} + t^{n-2} + t^{n-3}$. So it suffices to show that every element in the kernel of $\bar{\varphi}$ is represented by some g_n in the kernel of φ . Since n and $n-4$ are 0 and $2 \pmod{6}$, there are g of degree n and $n-4$ in the kernel of φ , and if we can show that the kernel of $\bar{\varphi}$ is spanned by the images of these 2 elements we'll be done. So it's enough to show that the image of $\bar{\varphi}$ has dimension ≥ 4 . But Lemma 1.9 tells us that φ maps $t^{n-1}, t^{n-2}, t^{n-3}, t^{n-5}$ to polynomials of degrees $n-2, n-4, n-5, n-6$, completing the proof. \square

Theorem 3.5 Let A, B, C and D be $1, t^6 + t^5 + t^4 + t^3 + t^2 + t, t^2 + t$ and t^8 . Then if the $g_n, n \equiv 0$ or $2 \pmod{6}$, are chosen as in Lemma 3.4:

- (a) $g_{12m} = (t^6 + t^5)^{2m} \cdot A + O(t^{12m-2})$.
- (b) $g_{12m+6} = (t^6 + t^5)^{2m} \cdot B + O(t^{12m})$.
- (c) $g_{12m+2} = (t^6 + t^5)^{2m} \cdot C + O(t^{12m})$.
- (d) $g_{12m+8} = (t^6 + t^5)^{2m} \cdot D + O(t^{12m+4})$.

Proof $(t^6 + t^5)^{2m} = t^{12m} + O(t^{12m-2})$, while $(t^6 + t^5)^{2m}(t^2 + t) = t^{12m+2} + t^{12m+1} + O(t^{12m})$. So (a) and (b) of Lemma 3.4 give us (a) and (c). In like manner, (d) for even and odd m follows from (c) and (d) of Lemma 3.4, while (b) for $m \equiv 0, 1, 2$ and $3 \pmod{4}$ follows from (e), (f), (g) and (h) of that lemma. Suppose for example that $n = 12m + 6$ and $m = 4k + 3$, so that $n = 48k + 42$. Then $(t^6 + t^5)^{2m}B = (t^6 + t^5)^{8k}(t^6 + t^5)^6B = t^{48k}(t^{42} + t^{41} + t^{38} + t^{37}) + O(t^{48k+36}) = t^n + t^{n-1} + t^{n-4} + t^{n-5} + O(t^{n-6})$. By Lemma 3.4(h) this is $g_n + O(t^{n-6}) = g_{12m+6} + O(t^{12m})$. \square

4 $N2, N2a$ and $N2b$. The structure of K

Recall that $M(\text{odd}) \subset Z/2[r]$ consists of the $(r^2 + r)g(r^2)$, g in $Z/2[t]$. $M(\text{odd})$ is stable under multiplication by r^2 , and in particular is a $Z/2[G^2]$ -module.

Definition 4.1 $N2$ is the (free rank 5) $Z/2[G^2]$ -submodule of $M(\text{odd})$ generated by the u_0, u_1, u_2, u_4 and u_5 of Lemma 2.6.

Lemma 4.2 Fix $m \geq 0$ and let L and L^* be as in Definition 2.7. The kernels of $(U + I)^2$ acting on L^* and its subspace L are the same.

Proof The proof of Theorem 2.10 shows that the dimension of the second kernel is $\geq 4m + 4$. But the kernel of $U + I : L^* \rightarrow L^*$ is just the K_m of Theorem 2.10, and the proof of Theorem 2.11 produces a basis of K_m with $2m + 2$ elements. So the dimension of the first kernel is $\leq 2(\text{the dimension of } K_m) = 4m + 4$. \square

Theorem 4.3 The kernel, K , of $U + I : M(\text{odd}) \rightarrow M(\text{odd})$ is a subspace of $N2$. So if $g_n, n \equiv 0$ or $2 \pmod{6}$, are as in Corollary 2.12 and $f_n = (r^2 + r)g_n(r^2)$, then each f_n is in $N2$.

Proof If f is in K , f is in L^* for some $m \geq 0$. Since $(U + I)f = 0$, Lemma 4.2 tells us that f is in L . But by definition $N2$ contains L for every m . \square

Definition 4.4 $N1$ is the $Z/2[G^2]$ -submodule of $N2$ generated by $u_2 = G$. Note that $G^k, k > 0$ and odd, are a basis of $N1$.

Definition 4.5 J_1, J_7, J_3 and J_9 are F, F^2G, F^4G and F^8/G .

Note that mod $N1$, $J_3 = (F + G)^8/G = F(F + G)^2$. So J_3 , like J_1 , J_7 and J_9 lies in $M(\text{odd})$.

Lemma 4.6 *G, J_1, J_3, J_7 and J_9 generate the same $Z/2[G^2]$ -submodule of $M(\text{odd})$ as do G, F, F^2G, F^3 and F^4G . This submodule is in fact $N2$. It follows that J_1, J_3, J_7 and J_9 are a $Z/2[G^2]$ basis of $N2/N1$.*

Proof $J_1 = F, J_7 = F^2G, J_9 = F^4G$ and $J_3 = F^3 + FG^2$ mod $N1$, giving the first result. Also, mod $N1$, $u_0, u_4, u_1 + u_4$ and $u_5 + u_4$ are $F, F^2G, F^3 + FG^2$ and $F^4G + FG^2$. So the second result follows. \square

We have defined J_k for k in $\{1, 3, 7, 9\}$. We extend the definition to all $k > 0$ and prime to 10 by taking J_{k+10} to be G^2J_k . Lemma 4.6 then shows that the J_k form a $Z/2$ -basis of $N2/N1$.

We will use results from [4] to obtain level 5 analogs of the level 3 theorems of [3]. To that end we need to compare the subspace K of $N2$ appearing in Theorem 4.3 with a certain space $N2a$ appearing in a direct sum decomposition of $N2/N1$.

Definition 4.7 *χ is the mod 20 Dirichlet character taking 1, 3, 7, 9 to 1 and 11, 13, 17, 19 to -1 . $N2a$ is spanned by the J_k in $N2/N1$ with $\chi(k) = 1$. $N2b$ is spanned by the J_k in $N2/N1$ with $\chi(k) = -1$.*

Note that $N2a$ is a $Z/2[G^4]$ -submodule of $N2/N1$ with basis $\{J_1, J_3, J_7, J_9\}$, that $N2b$ is a $Z/2[G^4]$ -submodule with basis $\{J_{11}, J_{13}, J_{17}, J_{19}\}$ and that $N2/N1 = N2a \oplus N2b$. Composing the inclusion $K \subset N2$ of Theorem 4.3 with the obvious projection $N2 \rightarrow N2a$ coming from the direct sum decomposition, we get a map $K \rightarrow N2a$. We shall show that this map is bijective—a level 5 analog to the level 3 result proved in the last paragraph of section 3 of [3].

Definition 4.8 *An element of $N2/N1$ is $O^*(J_k)$ if it is a sum of J_i with $i \leq k$.*

The proof of Lemma 4.6 shows that mod $N1$, u_0, u_1, u_4 and u_5 are $J_1, J_7 + J_3, J_7$ and $J_{11} + J_9 + J_7$. So the images of $G^n u_i$ in $N2/N1$ are $O^*(J_{10n+1}), O^*(J_{10n+7}), O^*(J_{10n+7})$ and $O^*(J_{10n+11})$ according as i is 0, 1, 4 or 5.

Lemma 4.9 *Suppose h is in $Z/2[t]$ and $f = (r^2 + r)h(r^2)$ is in $N2$.*

- (a) *If degree $h \leq 6m + 4$, the image of f in $N2/N1$ is $O^*(J_{10m+7})$.*
- (b) *If degree $h \leq 12m$, the image of f in $N2/N1$ is $O^*(J_{20m+1})$.*

Proof Write f as a sum of $G^n u_i$, i in $\{0, 1, 2, 4, 5\}$. Then h is the sum of the corresponding $(t^6 + t^5)^n, (t^6 + t^5)^n \cdot t, (t^6 + t^5)^n \cdot t^2, (t^6 + t^5)^n(t^4 + t^3)$ and $(t^6 + t^5)^n(t^5 + t^3)$. The degrees of these elements are distinct. So in the situation of (a), each of the elements has degree $\leq 6m + 4$, and each n that appears is

$\leq m$, with strict inequality when $i = 5$. The paragraph following Definition 4.8 then gives the result. Similarly, in the situation of (b), each element in the sum for h has $n \leq 2m$ with inequality when $i = 1, 2, 4$ or 5 , and again we use the paragraph following Definition 4.8. \square

Theorem 4.10 *Let the g_n of Corollary 2.12, $n \equiv 0$ or 2 (6), be chosen as in Theorem 3.5, and let $f_n = (r^2 + r)g_n(r^2)$. Recall that the f_n are a $\mathbb{Z}/2$ -basis of K . Consider the composite map $K \subset N2 \rightarrow N2a$ described after Definition 4.7. Then:*

- (a) f_{12m} maps to $J_{20m+1} + O^*(J_{20m-11})$.
- (b) f_{12m+6} maps to $J_{20m+3} + O^*(J_{20m+1})$.
- (c) f_{12m+2} maps to $J_{20m+7} + O^*(J_{20m+3})$.
- (d) f_{12m+8} maps to $J_{20m+9} + O^*(J_{20m+7})$.
- (e) The map $K \subset N2 \rightarrow N2a$ is bijective.

Proof It's enough to prove (a), (b), (c), (d). For if they hold, our map takes a basis of K to a basis of $N2a$.

- (a) $g_0 = 1$ and so $f_0 = r^2 + r = F + G$ with image J_1 . Suppose $m > 0$. By Theorem 3.5, $g_{12m} = (t^6 + t^5)^{2m} + g^*$ with degree $g^* \leq 6(2m - 1) + 4$. Let $f^* = (r^2 + r)g^*(r^2)$. Then $f_{12m} = G^{4m}u_0 + f^*$. Since f_{12m} is in $N2$, so is f^* . The image of u_0 is J_1 . So the image of $G^{4m}u_0$ is J_{20m+1} , and Lemma 4.9(a) shows that the image of f^* in $N2/N1$ is $O^*(J_{20m-3})$. Since J_{20m-3}, J_{20m-7} and J_{20m-9} are all in $N2b$, the image of f^* in $N2a$ is in fact $O^*(J_{20m-11})$.
- (c) By Theorem 3.5, $g_{12m+2} = (t^6 + t^5)^{2m}(t^2 + t) + g^*$ with degree $g^* \leq 12m$. Let $f^* = (r^2 + r)g^*(r^2)$. Then $f_{12m+2} = G^{4m}(u_2 + u_1) + f^*$, and once again f^* is in $N2$. The paragraph following Definition 4.8 shows that the image of u_1 is $J_7 + J_3$. So the image of $G^{4m}u_1$ is $J_{20m+7} + J_{20m+3}$. Also, Lemma 4.9(b) shows that the image of f^* is $O^*(J_{20m+1})$.
- (b) By Theorem 3.5, $g_{12m+6} = (t^6 + t^5)^{2m}(t^6 + t^5 + t^4 + t^3 + t^2 + t) + g^*$ with degree $g^* \leq 12m$. Let $f^* = (r^2 + r)g^*(r^2)$. Then $f_{12m+6} = G^{4m}(G^2u_0 + u_4 + u_2 + u_1) + f^*$, and once again f^* is in $N2$. The image of $G^{4m+2}u_0$ in $N2/N1$ is J_{20m+11} which lies in $N2b$. The paragraph following Definition 4.8 shows that the image of $u_4 + u_1$ is J_3 . So the image of $G^{4m}(u_4 + u_1)$ is J_{20m+3} . And as in (c), the image of f^* is $O^*(J_{20m+1})$.
- (d) By Theorem 3.5, $g_{12m+8} = (t^6 + t^5)^{2m}(t^8 + t^3) + g^*$ with degree $g^* \leq 12m + 4$. Let $f^* = (r^2 + r)g^*(r^2)$. Observing that $t^8 + t^3 = (t^6 + t^5)(t^2 + t + 1) + (t^5 + t^3)$, we find that $f_{12m+8} = G^{4m}(G^2(u_2 + u_1 + u_0) + u_5) + f^*$, so that f^* is in $N2$. The image of $u_1 + u_0$ in $N2/N1$ is $J_7 + J_3 + J_1$, and the image of $G^{4m+2}(u_2 + u_1 + u_0)$ therefore lies in $N2b$. Since the image of u_5 in $N2/N1$ is $J_{11} + J_9 + J_7$, the image of $G^{4m}u_5$ is $J_{20m+11} + J_{20m+9} + J_{20m+7}$ which projects to $J_{20m+9} + J_{20m+7}$ in $N2a$. Lemma 4.9(a) shows that the image of f^* is $O^*(J_{20m+7})$ completing the proof.

\square

5 The action of T_p and the main theorem

Following the ideas sketched in the introduction we use Theorems 4.3 and 4.10(e) to derive a result about a certain Hecke algebra in level $\Gamma_0(5)$. We refer extensively to [4]. Instead of r being an indeterminate it is now the explicit element $\sum_{n>0}(x^{n^2} + x^{2n^2} + x^{5n^2} + x^{10n^2})$ of $Z/2[[x]]$. Then $Z/2[r]$ is a subspace of $Z/2[[x]]$, and Theorem 1.11 of [4] shows that it is the space, M , of mod 2 modular forms of level $\Gamma_0(5)$. That theorem also shows that the subspace $M(\text{odd})$ of M consisting of odd power series lying in M is just the $M(\text{odd})$ of the present paper, spanned by the $(r^2 + r)r^{2n}$.

Now for $p \neq 2$ or 5 we have formal Hecke operators $T_p : Z/2[[x]] \rightarrow Z/2[[x]]$. They commute and stabilize M and $M(\text{odd})$; see Theorem 1.14 of [4] and the paragraph preceding it.

Definition 5.1 $U_5 : Z/2[[x]] \rightarrow Z/2[[x]]$ takes $\sum c_n x^n$ to $\sum c_{5n} x^n$.

Lemma 5.2 U_5 commutes with the T_p and stabilizes M and $M(\text{odd})$.

Proof It's enough to show that U_5 stabilizes the space spanned by the r^i with $0 \leq i \leq 2m$. We argue as in the proof of Theorem 1.14 of [4], using the classical Hecke operator $\sum c_n x^n \rightarrow \sum c_{5n} x^n$ on weight $4m$ holomorphic modular forms of level $\Gamma_0(5)$. \square

Lemma 5.3 $F = \sum_{n \text{ odd}, n>0} x^{n^2}$, and $G = \sum_{n \text{ odd}, n>0} x^{5n^2}$.

Proof See Theorem 1.12 of [4] and the paragraph preceding it. \square

Lemma 5.4 $U_5 : M \rightarrow M$ is the map U of Definition 1.3.

Proof Lemma 5.3 and the definition of U_5 show that $U_5(Gf) = FU_5(f)$. So $U_5 : M \rightarrow M$ like U is semi-linear, and it's enough to show that they agree on the basis $1, r, r^2, r^3, r^4, r^5$ of $Z/2[r]$ as $Z/2[G]$ -module. One sees directly from the definitions that $U_5(r) = r$. Then U_5 and U each fix $1, r, r^2, r^4$ and r^8 . Since $r^5 = r^8 + G((r^2 + r + 1))$, we may use semi-linearity to see that $U_5(r^5) = U(r^5)$. Then $U_5(r^{10}) = U(r^{10})$, and since $G(r^4 + r^3) = r^{10} + r^8$ another application of semi-linearity shows that $F \cdot U_5(r^3) = F \cdot U(r^3)$.

Recall now that $N2$ and $N1$ are the $Z/2[G^2]$ -submodules of $M(\text{odd})$ with bases $\{G, F, F^2G, F^3, F^4G\}$ and $\{G\}$, and that $N2a$ and $N2b$ are the subspaces of $N2/N1$ spanned by the J_k in $M(\text{odd})$ with $\chi(k) = 1$ and -1 respectively. $N2$ and $N1$ also appear in Definition 1.15 of [4] and coincide with the $N2$ and $N1$ just described. Also, the J_k with $(k, 10) = 1$ appear in Definitions 1.16 and Theorem 1.17 of [4]. Those definitions, in terms of F and G , show that the J_k are just the J_k in our section 4. It follows that the subspaces $N2a$ and $N2b$ of

$N2/N1$ appearing in the paragraph following the proof of Lemma 2.13 of [4] are the $N2a$ and $N2b$ of our section 4. \square

Lemma 5.5 *Let K be the kernel of $U_5 + I$ acting on the space $M(\text{odd})$ of odd mod 2 modular forms of level $\Gamma_0(5)$. Let $N2, N1, N2a$ and $N2b$ be as in [4]. Then $K \subset N2$ and the composition of $N2 \rightarrow N2/N1$ with the projection map $N2/N1 = N2a \oplus N2b \rightarrow N2a$ maps K bijectively to $N2a$.*

Proof We have seen that $M(\text{odd})$ is just the subspace of $Z/2[r]$ spanned by the $(r^2 + r)r^{2n}$. Furthermore, by Lemma 5.4, K is the kernel of $U + I$ acting on this space. The results now follow from Theorem 4.3, Theorem 4.10(e), and the identification of the $N2, N1, N2a$ and $N2b$ of [4] with the $N2, N1, N2a$ and $N2b$ defined in this paper. \square

Now Lemma 5.2 shows that the $T_p : Z/2[[x]] \rightarrow Z/2[[x]]$, $p \neq 2$ or 5 , stabilize not only $M(\text{odd})$, but also the K of Lemma 5.5. Also by Theorem 2.19 of [4] and the remark following Theorem 1.17 of [4], these T_p also stabilize $N2$ and $N1$, and therefore act on $N2/N1 = N2a \oplus N2b$. Since $\chi(3) = \chi(7) = 1$, Corollary 2.18 of [4] shows that T_3 and T_7 stabilize $N2a$ and $N2b$.

Lemma 5.6 *The bijection $K \rightarrow N2a$ of Lemma 5.5 preserves the action of T_3 and T_7 .*

Proof It suffices to show that the projection map $N2a \oplus N2b \rightarrow N2a$ preserves the action of T_3 and T_7 . But T_3 and T_7 stabilize both $N2a$ and $N2b$. \square

Now let $pr : N2 \rightarrow Z/2[[x]]$ be the map $\sum c_n x^n \rightarrow \sum_{(n,5)=1} c_n x^n$. This map annihilates $N1$ and gives a map $pr : N2/N1 \rightarrow Z/2[[x]]$. Let $D = pr(J_1) = \sum_{(n,10)=1, n>0} x^{n^2}$.

In section 2 of [4] we showed that pr maps $N2a$ bijectively to a $Z/2[G^4]$ -submodule of $Z/2[[x]]$, denoted by W_a , generated by $D, D^8/G, D^2G$ and D^4G . Furthermore T_3 and T_7 stabilize W_a , and $pr : N2a \rightarrow W_a$ evidently preserves the action of T_3 and T_7 . We conclude that the composite map $K \rightarrow N2a \rightarrow W_a$ is a bijection preserving the action of T_3 and T_7 . Note also that this bijection maps the element $r^2 + r = F + G$ of K to D .

We will now use a deep result from [4] to prove the following main theorem.

Theorem 5.7 *Let K be as in Lemma 5.5. Then there are $m_{i,j}$ in K such that:*

- (a) $m_{0,0} = r^2 + r = F + G$.
- (b) $T_3(m_{i,j}) = m_{i-1,j}$ or 0 according as $i > 0$ or $i = 0$.
- (c) $T_7(m_{i,j}) = m_{i,j-1}$ or 0 according as $j > 0$ or $j = 0$.
- (d) The $m_{i,j}$ are a $Z/2$ -basis of K .

Proof In view of the bijection of K with W_a , preserving the action of T_3 and T_7 , it suffices to prove the above result with K and $F + G$ replaced by W_a and D . The result for W_a is precisely Corollary 5.13 of [4]. \square

Now there is an action of $Z/2[X, Y]$ on K with X and Y acting by T_3 and T_7 . Theorem 5.7 shows that (X, Y) acts “locally nilpotently”, i.e., each f in K is annihilated by some power of (X, Y) . So we get an action of $Z/2[[X, Y]]$, with X and Y acting by T_3 and T_7 .

Theorem 5.8 *The above action is faithful. Furthermore if $p \neq 2$ or 5 then $T_p : K \rightarrow K$ is multiplication by some element of the maximal ideal (X, Y) of $Z/2[[X, Y]]$.*

Proof The first result is an easy consequence of Theorem 5.7. If $p \neq 2$ or 5 , T_p commutes with T_3 and T_7 and so is $Z/2[[X, Y]]$ -linear. Theorem 5.7 then shows (see the proof of Theorem 4.16 of [2]) that $T_p : K \rightarrow K$ is multiplication by some u in $Z/2[[X, Y]]$. Since $T_p(m_{0,0}) = T_p(F + G) = 0$, u is in (X, Y) . \square

Finally, since the T_p , $p \neq 2$ or 5 , act on K , we have a “completed shallow Hecke algebra”, $HE(K)$, attached to K . Theorem 5.8 tells us that $HE(K)$ is a power series ring in T_3 and T_7 . At the same time the action of these T_p on $N2/N1$ gives rise to a completed shallow Hecke algebra $HE(N2/N1)$. Theorem 7.2 of [4] tells us that $HE(N2/N1)$ is a power series ring in T_3 and T_7 with an element of square 0 adjoined. Arguing as in the final paragraph of [3] we find:

Theorem 5.9 *There is an isomorphism $(HE(N2/N1))_{red} \rightarrow HE(K)$ taking T_p to T_p for each $p \neq 2$ or 5 .*

References

- [1] Monsky P. (2015), “A characteristic 2 polynomial recursion.” mathoverflow.net question 214621.
- [2] Monsky P. (2015), “A Hecke algebra attached to mod 2 modular forms of level 3.” arXiv:1508.07523 [math.NT].
- [3] Monsky P. (2016), “A characteristic 2 recurrence related to U_3 with a Hecke algebra application.” arXiv:1603.03910 [math.NT].
- [4] Monsky P. (2016), “A Hecke algebra attached to mod 2 modular forms of level 5.” arXiv:1610.07085 [math.NT].